Clay County Communications, LLC
216 Main Street
P.O. Box 240
Everly, IA 51338

February 1, 2010

Marlene H. Dortch, Secretary
Office of the Secretary
Federal Communications Commission
445 12th Street, SW
Suite TW-A325
Washington, D.C. 20554

RE: EB Docket No. 06-36
Annual CPNI Certification

Dear Ms. Dortch:

In accordance with FCC Enforcement Advisory DA 10-91, issued on January 15, 2010, attached is the annual CPNI certification filing covering the year of 2009, pursuant to 47 C.F.R § 64.2009(e), for Clay County Communications, LLC.

Sincerely,

Roxanne White
Executive Vice President

Attachment

cc: Best Copy and Printing, Inc.
445 12th Street
Suite CY-B402
Washington, D.C. 20554
Email: FCC2BCPIWEB.COM

Annual 47 C.F.R. § 64.2009(e) CPNI Certification Template

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2010 covering the prior calendar year 2009

1. Date filed: February 1, 2010

2. Name of company(s) covered by this certification:

   Clay County Communications, LLC

3. Form 499 Filer ID: *826488*

4. Name of signatory: Roxanne White

5. Title of signatory: Executive Vice President

6. Certification:

I, Roxanne White, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. *See* 47 C.F.R. § 64.2001 *et seq.*

Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements (including those mandating the adoption of CPNI procedures, training, recordkeeping, and supervisory review) set forth in section 64.2001 *et seq.* of the Commission's rules.

The company has not taken actions (*i.e.*, proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year.

The company has not received customer complaints in the past year concerning the unauthorized release of CPNI.

The company represents and warrants that the above certification is consistent with 47. C.F.R. § 1.17 which requires truthful and accurate statements to the Commission. The company also acknowledges that false statements and misrepresentations to the Commission are punishable under Title 18 of the U.S. Code and may subject it to enforcement action.

Signed 

Attachment: Accompanying Statement explaining CPNI procedures

ATTACHMENT

OPERATING PROCEDURES FOR ENSURING COMPLIANCE WITH CPNI RULES

Clay County Communications, LLC (the "Company") has implemented the following procedures to ensure that it is compliant with Part 64 of Title 47 of the Code of Federal Regulations, Subpart U – Customer Proprietary Network Information (CPNI), § 64.2001 through § 64.2011.

Compliance Officer

The Company has appointed a CPNI Compliance Officer. The Compliance Officer is responsible for ensuring that the Company is in compliance with all of the CPNI rules. The Compliance Officer is also the point of contact for anyone (internally or externally) with questions about CPNI.

Employee Training:

The Compliance Officer arranges for the training of all employees on an annual basis, and more frequently as needed. Any new employee is trained when hired by the Company. The training includes, but is not limited to, when employees are and are not authorized to use CPNI, and the authentication methods the company is using. The detail of the training can differ based on whether or not the employee has access to CPNI.

After the training, all employees are required to sign a certification that they have received training on the CPNI rules, that they understand the Company's procedures for protecting CPNI and they understand the Company's disciplinary process for improper use of CPNI. Each employee knows where the CPNI Manual is located with all of the rules and regulations, and it is easily accessible to all employees.

Employees are instructed that if they ever have any questions regarding the use of CPNI, if they are aware of CPNI being used improperly by anyone or if they encounter someone other than the authorized person listed on an account trying to access CPNI that they should contact the Compliance Officer immediately. The Compliance Officer will then determine what action needs to be taken.

Disciplinary Process

The Company has established a specific disciplinary process for improper use of CPNI. The disciplinary action is based on the type and severity of the violation and could include any or a combination of the following: retraining the employee on CPNI rules, notation in the employee's personnel file, formal written reprimand, suspension or termination.

The disciplinary process is reviewed with all employees.

A copy of the Company's disciplinary process is kept in the Company Manual.

Customer Notification and Request for Approval to Use CPNI

The Company has provided notification to its customers of their CPNI rights but has not asked for approval to use their CPNI. The Company's position is that all customers have opted out. A copy of the notification is also provided to all new customers that sign up for service.

If the Company wants to solicit the customer for other Company services, the Company will use the notice requirements specific to one-time use of CPNI for the duration of the call. For example, at the time of install or service an employee may ask customers if they would like to hear about any other services offered by our Company. The employee does this by providing the

oral notice to obtain limited, one-time use of CPNI, which gives the customer the opportunity to opt in or opt out at that time. After the conclusion of the one-time opting in discussion, the customer's status will change back to opted-out.

Marketing Campaigns

The Company does not use CPNI for marketing purposes. If, in the future, it conducts any marketing campaigns, the Company will first establish a supervisory review process and a process for maintaining a record of any marketing campaign of its own, or its affiliates.

Authentication

The Company does not disclose any CPNI until the customer has been appropriately authenticated as follows:

In-office visit - the customer must provide a valid photo ID matching the customer's account information.

Customer-initiated call – the customer is authenticated by providing the last four digits of his/her social security number as the answer to his/her question and must be listed as a contact on the account.

If the customer wants to discuss call detail information, the following guidelines are followed:

- If the customer can provide all of the call detail information (telephone number called, when it was called, and the amount of the call) necessary to address the customer's issue, the Company will continue with its routine customer care procedures.

- If the customer cannot provide all of the call detail information to address the customer's issue, the Company will: (1) call the customer back at the telephone number of record, (2) send the information to the address of record, or (3) ask the customer to come into the office and provide a valid photo ID.

Notification of Account Changes

The Company promptly notifies customers whenever a change is made to any of the following:

- Address of record
- Account status
- Authorized users

The notification to the customer will be made by a Company written notification to the customer's address of record. The company's billing software generates a letter based on the above account changes.

Notification of Breaches

Employees will immediately notify the Compliance Officer of any indication of a breach. If it is determined that a breach has occurred, the Compliance Officer will do the following:

- Notify the United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI) as soon as practicable, but in no event later than 7 business days after determination of the breach. The notification will be via the FCC link at http://www.fcc.gov/eb/cpni.

- Notify customers only after 7 full business days have passed since notification to the USSS and the FBI, unless the USSS or FBI has requested an extension.

- If there is an urgent need to notify affected customers or the public sooner to avoid immediate and irreparable harm, it will be done only after consultation with the relevant investigating agency.

- Maintain a record of the breach, the notifications made to the USSS and FBI, and the notifications made to customers. The record should include dates of discovery and notification, a detailed description of the CPNI that was the subject of the breach, and the circumstances of the breach.

- Include a summary of the breach in the annual compliance certificate filed with the FCC.

Miscellaneous

The Company takes reasonable measures to discover and protect against activity that is indicative of pretexting, as well as any other signs of unauthorized access to CPNI. Employees are instructed to notify the CPNI Compliance Officer immediately of any unusual or suspicious activity who will then determine what action needs to be taken.

Annual Certification

The Compliance Officer will ensure that a Compliance Certification is filed with the FCC by March 1 of each year for data pertaining to the previous calendar year.

Record Retention

The Company retains all information regarding CPNI. General CPNI information is located in the Company's CPNI Manual, and personal information concerning accounts is in a separate file in our billing department. Below is a listing of our minimum record retention guidelines:

- CPNI notification and records of approval – two years
- Breaches – two years
- Annual certification – seven years
- Employee training certification – two years
- All other information – two years